AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions and listings of claims in the application.

LISTING OF CLAIMS

1-19. (cancelled)

20. (New) In a mobile platform, a security system for monitoring an onboard communication system communicating with a terrestrial-based system over an intermittent link, the security system comprising:

an onboard network accessible to a plurality of users;

an intrusion detection system connected to the onboard network;

an onboard security management system responsive to the intrusion detection system for initiating an action to stop intrusion based on a set of policies; and

wherein, if an update is necessary, the policies being updated during the time that the intermittent link has connection.

21. (New) The security system as recited in claim 20, wherein initiating the action to stop intrusion comprises sending a warning message to the user.

22. (New) The security system as recited in claim 20, wherein initiating the action to stop intrusion comprises disconnecting the user's access to the onboard network.

23. (New) The security system as recited in claim 20, wherein the onboard security management system further operates to provide an alert message to the terrestrial-based system when an intrusion event is detected.

24. (New) The security system as recited in claim 20, wherein the onboard security management system further operates to install a network traffic blocking filter on one of a plurality of user access points of the onboard network.

25. (New) The security system as recited in claim 20, wherein the action to stop intrusion is directed to a specific one of a plurality of user access points of the onboard network.

26. (New) The security system recited in claim 20, wherein the onboard security manager maintains an indicator of a current operational state of each one of a plurality of network user access points of the onboard network.

27. (New) The security system recited in claim 26, wherein the indicator indicates one of:

a normal operational state;

a suspect operational state wherein an intrusion event is suspected; and

a disconnect state in which access by a user of a specific access point on the onboard network is prevented.

28. (New) In a mobile platform, a security system for monitoring an onboard communication system communicating with a terrestrial-based system over an intermittent link, the security system comprising:

an onboard network accessible to a plurality of users;

an intrusion detection system connected to the onboard network for detecting if a potential intrusion event has occurred;

an onboard security management system responsive to the intrusion detection system for initiating an action to address the potential intrusion event, based on a set of security policies; and

wherein the action can be directed to at least a selected one of a plurality of user access points on the onboard network.

29. (New) The security system as recited in claim 28, wherein if an update to the set of policies is necessary, the policies are updated during the time that the intermittent link has connection with the terrestrial-based system.

30. (New) The security system as recited in claim 28, wherein the onboard security manager notifies the terrestrial-based system when the potential intrusion event is detected.

31. (New) The security system as recited in claim 28, wherein the action comprises preventing access to the onboard network from a selected one or more of the user access points from the onboard network.

32. (New) The security system as recited in claim 28, wherein the onboard security manager maintains an indicator of a current operational state of each one of the plurality of network user access points of the onboard network.

33. (New) The security system as recited in claim 32, wherein the indicator indicates whether at least one of the following conditions is present:

a normal state of operational for the onboard network;

a suspect operational state wherein an intrusion event is suspected; and

a disconnect state in which access by a user of a specific one of the user access points is being prevented.

34. (New) In a mobile platform, a security system for monitoring an onboard communication system communicating with a terrestrial-based system over an intermittent link, the security system comprising:

an onboard network accessible to a plurality of users;

an intrusion detection system for monitoring the onboard network for detecting if a potential intrusion event has occurred;

an onboard security management system responsive to the intrusion detection system for initiating an action to address the potential intrusion event, based on a set of security policies, the action able to be directed to at least a selected one of a plurality of user access points on the onboard network; and

wherein the action includes one of:

notifying a particular user on the onboard network that a suspected intrusion event has occurred; or

blocking access by the particular user to the onboard network.

35. (New) The security system recited in claim 34, wherein the onboard security management system receives updates to said security policies from the terrestrial-based system while said intermittent link is operational.

36. (New) The security system recited in claim 34, wherein the onboard security management system notifies the terrestrial-based system that a potential intrusion event has occurred.

37. (New) The security system recited in claim 34, where the action taken by the onboard security management system further includes installing a network traffic blocking filter on said user access point on which a potential intrusion event has occurred.

38. (New) A method for monitoring an onboard network on a mobile platform, in which the onboard network is in intermittent communication with a terrestrial-based system, the method comprising:

providing a plurality of network access points to users on the mobile platform;

monitoring the onboard network to detect for an intrusion event;

using a security management system onboard the mobile platform, and responsive to notification of an intrusion event, to initiate a security action to address the intrusion event, in accordance with a set of security policies.

39. (New) The method recited in claim 38, further comprising updating the security policies while the onboard network is in communication with the terrestrial-based system.